14th Annual Miami-Dade Healthcare Preparedness Coalition
Cyber Attack Considerations for Healthcare
April 10, 2024
1:30PM-3:00PM

Kimberly Smoak

Deputy Secretary

Health Care Policy and Oversight

Agency for Health Care Administration

Cyber Security – Development of Emergency Preparedness Plans

- Develop an all-hazards approach.
  - focus on identifying hazards
  - developing capacities and capabilities
- Access to and maintain medical records.
- Federal regulations require providers to plan for situations in which they may not be able to have access to their current format (i.e. electronic records during cyberattack).

What measures to you have in place for security?

- Role based access control?
- Multi-factoral authentication ?
- Vulnerability assessment?
- Penetration testing? Source: www.riomed.com

Training

- What training do your staff have to prevent phishing and other attacks that can impact the security of data, including patient information?
- How do you monitor that training (example: fake phishing emails to determine if staff report)?
- What is your plan should there be a possible attack?

Cybersecurity's Primary Opponents: Phishing and Ransomware

- No matter how strong the locks are on your front door, if someone lets the criminals in, they don't work. This is what phishing attacks are attempting to accomplish.
- The most common way for ransomware to breach a network is phishing.
  - Hospitals are a primary target for these attacks, and the extorted payments from victims reach over **$1 billion in 2023 alone.**
- Provide a way to quickly and easily report suspicious emails.
- Tie in your anti-phishing program to your IT network team; this helps to prevent attacks in the future.
  - Create a culture of defending against phishing attacks-your users get attacked like this at home, too!

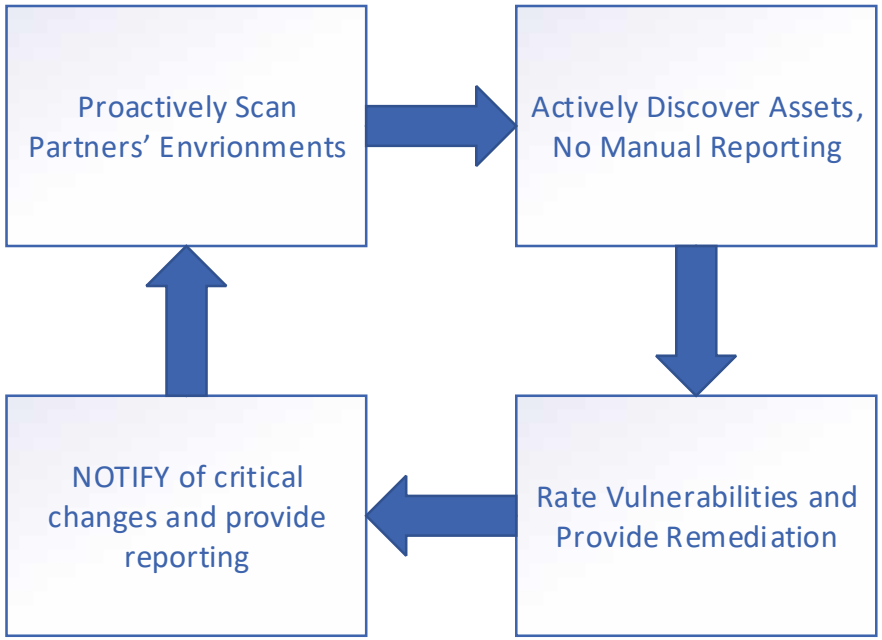
Impact of Breaches – Far More Than Dollars

- Statnews November 2023: “From 2016 to 2021, we estimate that ransomware attacks **killed between 42 and 67 Medicare patients.”**
- JAMA: The true number of deaths caused by ransomware attacks is likely even larger, when you include patients with other types of health insurance coverage.
- JAMA: “the annual number of ransomware attacks on health care delivery organizations more than doubled from 2016 to 2021”.
- JAMA: Ransomware attacks increase every year, with the healthcare industry a frequent target. These statistics are expected to be significantly higher in 2024 and future years.
- JAMA: It’s time “to view these types of attacks, ransomware attacks on hospitals, as **threat-to-life crimes**, not financial crimes,” said John Riggi, the national adviser for cybersecurity and risk at the American Hospital Association.

Internal Cybersecurity Cycle

Robust Cybersecurity Risk Management

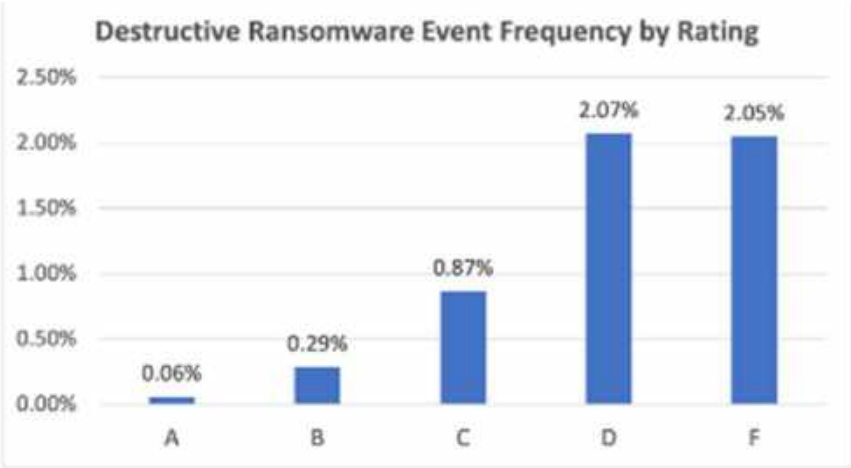
Cybersecurity Supply Chain is Critical to Protect Patient Data – Make it a Contract Requirement with Partners.

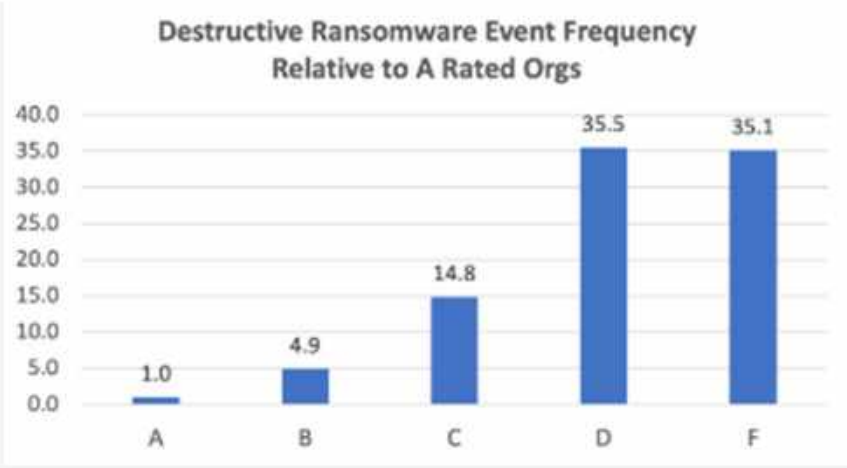


Prioritize Information Technology and Cybersecurity Risk Management at a Leadership Level. As part of critical operations, this helps to ensure a robust and efficient cybersecurity posture for the business.

Partner and Vendor Cyber Supply Chain

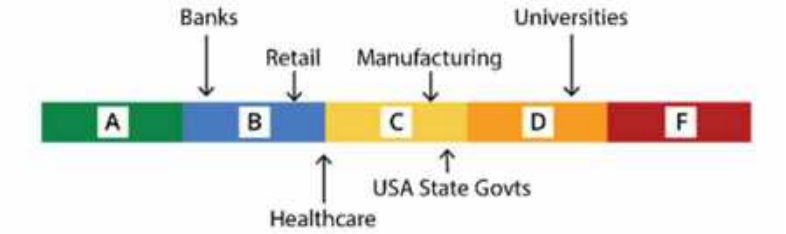
- The rating model is designed to achieve two objectives: be reflective of good cybersecurity hygiene as it manifests in the real world and to be strongly correlated with risk outcomes, such as destructive ransomware and the frequency of breach events.

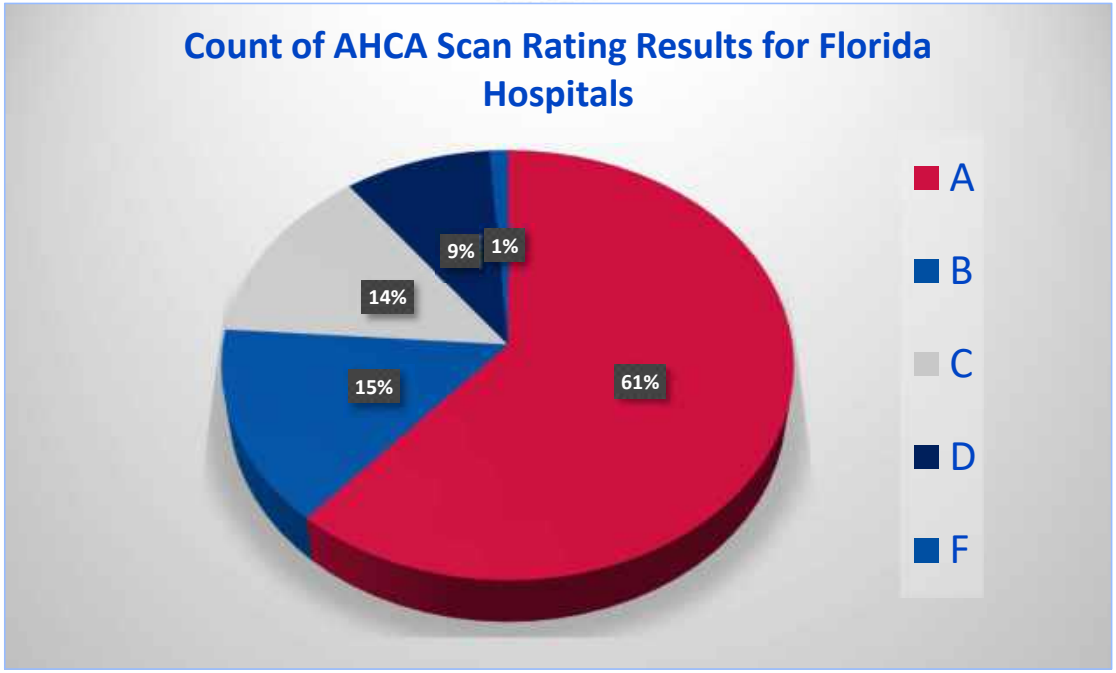




The Objective – Better Protection Against Ransomware

- This rating system utilizes federal (CVSS) rating for risk priority in addition to the asset's value (ex. PHI) and proximity to assets of high value. This provides better visibility into risk hygiene than just issue severity.





Kimberly R. Smoak, MSH, QIDP

(850) 412-4516 or (850) 559-8273
Kimberly.Smoak@ahca.myflorida.com